Board of Governors of the Federal Reserve System

REPORT ON THE BOARD'S IMPLEMENTATION OF CRITICAL INFRASTRUCTURE PROTECTION PHASE II

OFFICE OF INSPECTOR GENERAL

(A0007) March 2001

BOARD OF GOVERNORS
OF THE
FEDERAL RESERVE SYSTEM
WASHINGTON, D. C. 20551

OFFICE OF INSPECTOR GENERAL

March 30, 2001

Board of Governors of the Federal
Reserve System
Washington, DC 20551

Dear Members of the Board:

The Office of Inspector General has completed the second phase of its review of the implementation of the *Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63* (PDD 63) by the Board of Governors of the Federal Reserve System (Board). We conducted this review as part of a multiphased, governmentwide effort organized by the President's Council on Integrity and Efficiency (PCIE) and the Executive Council on Integrity and Efficiency (ECIE).[1] On September 29, 2000, we provided you an assessment of the Board's cyber-based infrastructure planning and assessment activities based on our first review phase. In an effort to continue providing timely feedback, we are issuing this second interim report which describes the status of the Board's physical infrastructure planning and assessment activities, including matters that we believe warrant the Board's attention.

BACKGROUND

Issued in May 1998, PDD 63 calls for a national effort to secure the nation's critical infrastructures within five years. Critical infrastructures are the physical and computer-based systems essential to the minimum operation of the economy and government, and include telecommunications, banking and finance, energy, transportation, and essential government services. Advances in information technology have caused the infrastructures to become increasingly automated and interdependent and have created new vulnerabilities to equipment failures, human error, weather, and terrorist attacks. To address these threats, PDD 63 requires that each government department and agency develop a plan to protect its own critical infrastructure, that includes

- identifying infrastructures essential to perform the agency's core mission,

[1] The President's Council on Integrity and Efficiency, established by executive order, dated March 26, 1981, is comprised of all Presidentially appointed inspectors general and certain government officials. The Executive Council on Integrity and Efficiency, comprised primarily of the inspectors general appointed by designated federal entity heads, was created by executive order on May 11, 1992. Both the PCIE and the ECIE have the same mission: to address integrity and efficiency issues that transcend individual government agencies and increase the professionalism and effectiveness of inspector general personnel throughout the government. I currently serve as Vice Chair of the ECIE.

- identifying possible threats and vulnerabilities,
- providing a strategy for mitigating associated risks, and
- establishing educational and awareness efforts.

The plan should be updated regularly and provide a basis for the agency to request funding and resources necessary to implement the enhancements required to achieve desired protection levels by the directive's May 2003 completion date. Planning for PDD 63 is linked to planning and assessment activities for emergency management and threat awareness contained in other presidential directives. [2]

OBJECTIVE, SCOPE, AND METHODOLOGY

Our overall objective during this review phase was to evaluate the adequacy of the Board's planning and assessment activities for protecting critical physical infrastructures. Our review focused primarily on the Board's internal operations but also included the Board's oversight and regulatory responsibilities. To accomplish our review objective, we interviewed Board officials and staff responsible for planning, performing, and overseeing infrastructure protection activities and reviewed pertinent documentation. Our review was conducted in accordance with generally accepted government auditing standards.

ANALYSIS AND OBSERVATIONS

Overall, the Board has taken substantial action to ensure that the Board, Reserve Banks, and state member banks incorporate the critical, physical infrastructure protection objectives of PDD 63 into their planning processes. We found that although the Board has not yet prepared a critical infrastructure protection plan, the Board is building on prior planning activities to implement a comprehensive and structured process that, when completed, should address the necessary elements of PDD 63 and other related directives. We also found that the Division of Reserve Bank Operations and Payment Systems (RBOPS) has implemented a strong oversight program to help ensure that Reserve Bank security and protection programs incorporate the directive's requirements. In addition, long-standing and recently updated guidance to state member banks issued by the Division of Banking Supervision and Regulation (BS&R) and the Federal Financial Institution Examination Council (FFIEC) addresses the provisions and intent of PDD 63. Each of these three areas is discussed in more detail below. We have no recommendations at this time for specific improvements, although we have identified three matters for the Board's attention as the planning effort continues. We believe that the success of the actions taken thus far will depend on the Board's continued support and resource commitments, as well as its attention to organizational issues and further coordination between the Board and Reserve Banks.

[2] Two such directives are: PDD 62: Protection Against Unconventional Threats to the Homeland and Americans Overseas, and PDD 67: Enduring Constitutional Government and Continuity of Government Operations.

Board Infrastructure

Since our Phase I report, the Board has taken several actions to manage and staff the planning and assessment activities associated with PDD 63. The Staff Director for Management was designated as the Board's Critical Infrastructure Assurance Officer (CIAO) and he subsequently established a Critical Infrastructure Assurance Task Force. The task force is responsible for addressing the coordination of infrastructure protection activities across Board divisions and combining these activities with other contingency and continuity of operations planning efforts. For example, the Board has completed a draft *Continuity of Operations Plan* that identifies the processes and procedures needed to support the Board's actions to recover and respond during and after a crisis situation. The draft plan, which includes the designation of personnel and job functions needed if the Board must move critical functions to a contingency site, will comprise one piece of the Board's overall critical infrastructure contingency plan.

The Board's approach of building on existing continuity of operations and recovery plans is different from the approach envisioned in PDD 63. The PDD 63 approach called on agency management to first specify their mission-essential infrastructures, possible threats and vulnerabilities, and the likelihood and extent of such risks, as a focus for developing a comprehensive strategy for mitigating those risks. We recognize the merits of the Board's decision to first update its existing recovery plans, building on the work that was done to prepare for Y2K. We were concerned, however, that physical security and protection measures would be planned and implemented without management first reaching an understanding of the Board's critical infrastructures and the underlying vulnerabilities and associated risks. Without such agreement, we believe it would be more difficult to assess the cost-effectiveness of particular security and protection processes. We noted that a vulnerability assessment of the Board's facilities was last conducted by the U. S. Secret Service, at our request, in 1988. The Division of Support Services (SS) used that report and subsequent guidelines provided in 1995 by the Department of Justice following the Oklahoma City bombing as a basis for physical security improvements. SS officials indicated, however, that some recommended security enhancements were not considered feasible by senior management because of concerns for the impact on Board's culture and differences of opinion regarding threat risks and vulnerabilities.

After we discussed this matter with the Staff Director for Management, he requested a new vulnerability assessment by the U. S. Secret Service to establish a fresh vulnerability and risk baseline for planning the Board's physical security enhancements. When the assessment is completed in May 2001, SS management plans to work with the task force and the Staff Director for Management to evaluate any recommendations and develop plans and proposals for the 2002-03 budget to implement any needed enhancements. We believe this process will help Board management reach an understanding of the Board's mission-critical infrastructures, threat risks, and vulnerabilities that should be the basis for the Board's physical security and protection program. This process, combined with the work on continuity of operations planning, should result in a planning effort that will meet the PDD 63 requirements and provide the Board with a multiyear strategy and program management plan that addresses information security assurance, critical infrastructure protection, continuity of operations, and threats of terrorism.

Board Oversight of Reserve Banks

The RBOPS Bank Protection Program (BPP) has incorporated the elements of PDD 63 into its evaluation of Reserve Bank protection programs through its oversight activities and consultative visits. The BPP oversight program assesses the adequacy of Reserve Bank security and protection programs in identifying critical assets, conducting vulnerability assessments, and mitigating risks to protect the facilities, personnel, and systems that comprise a Bank's critical infrastructures. For example, Reserve Bank security programs are reviewed for compliance with the requirements of Regulation H, which requires Reserve Banks to establish a security program to protect valuable assets by discouraging robberies, burglaries, and larcenies.[3] The security programs are also assessed for the effectiveness and efficiency of security operations in accordance with industry best practices. In conjunction with these oversight activities, BPP also works with other RBOPS sections to address security considerations in their reviews of Reserve Bank business functions and contingency planning activities.

In addition to its oversight activities, BPP builds partnerships with Reserve Banks through consultative visits that focus on the physical protection of the Bank's facilities. BPP staff believes that these consultative visits, which began in 2000, have been successful and well received by Reserve Banks because they provide Reserve Banks with an external assessment of their vulnerabilities and identify ways to mitigate risks. These assessments are similar to reviews by the U. S. Secret Service. BPP plans to conduct periodic consultative visits to all Federal Reserve facilities at a pace of about twelve assessments per year.

During our review, we found that RBOPS has broadened its protection philosophy beyond traditional criminal activities to reflect the changing nature and sophistication of terrorist threats. As part of this approach, BPP coordinates with federal law enforcement, intelligence, and emergency management agencies and serves as a central point for the collection of information relevant to Reserve Bank security. In addition, the RBOPS director informed us that the BPP manager is planning to meet with the Conference of First Vice Presidents in May 2001 to discuss areas where it may be important for Reserve Banks to be consistent in their critical infrastructure assessment approaches. The division's broadened philosophy to protect Federal Reserve System infrastructures from both traditional crimes and terrorist attacks is in keeping with the intent of PDD 63.

Board Oversight of Depository Institutions

Over the years, the banking regulatory agencies have developed examination procedures and guidance documents that address many of the elements of PDD 63 relating to critical physical infrastructure. For example, supervisory guidance contained in Regulation H and other FFIEC interagency policies requires financial institutions to develop and maintain security and protection programs and business continuity contingency plans that protect their physical infrastructures. Appendix D-2 of Regulation H was recently amended to incorporate, in accordance

[3] Regulation H contains general provisions for membership in the Federal Reserve System. Section 208.61(e) requires each Reserve Bank to develop and maintain a written security program for its main office and branches subject to review and approval by the Board. Section 208.60 describes a member bank's obligation to implement a security program and associated procedures.

with sections 501 and 505 of the Gramm-Leach-Bliley Act (GLB Act), *Interagency Guidelines Establishing Standards for Safeguarding Customer Information*. These guidelines, which are effective July 2001, address standards for developing and implementing administrative, technical, and physical safeguards for customer information records. They require financial institutions to establish an information security program to

- identify and assess the risks that may threaten customer information;
- develop and test policies and procedures to manage and control these risks;
- adjust the plan on a continuing basis to account for changes in technology, sensitivity of customer information, and internal and external threats to information security; and
- ensure involvement of senior management.

As with Regulation H, a common thread throughout other regulatory guidance are the PDD 63 concepts of critical assets identification, vulnerability assessment, and risk mitigation. In November 2000, for example, the FFIEC issued *Risk Management of Outsourced Technology Services*. This guidance requires that financial institutions conduct a risk assessment to identify, measure, monitor, and control the risks associated with outsourcing technology services. Risk assessment criteria include the criticality of services to the financial institution, contingency plans, and ongoing assessments. Other regulatory guidance focuses on contingency and disaster recovery planning and uses risk assessment and risk mitigation techniques to identify possible threats such as natural disasters, technical failures and disgruntled employees.

The Federal Reserve is participating in regulatory and public sector initiatives to encourage implementation of the critical infrastructure principals incorporated in PDD 63. In December 2000, the Federal Reserve sponsored a meeting of financial regulators to review the status of regulatory PDD 63 public sector initiatives and identify areas for further attention. The CIAO and Board staff are also working with the Department of Treasury's Office of Financial Institutions Policy to encourage financial sector implementation of the principles espoused in PDD 63 and the GLB Act.

Matters for the Board's Attention

At this time, we do not have any recommendations for specific actions by the Board or division management because of the substantial amount of work completed to date and the Staff Director for Management's commitment to developing the operational elements of the Board's overall critical infrastructure and contingency plan. We believe, however, that the ongoing planning effort may present challenges that could require the attention of the Board and particularly the Board Affairs Committee. Three such matters are listed below. As the planning process continues, we will work with the Staff Director through our participation in the task force and, upon request, we will provide additional information and analysis that may be useful in the ongoing planning process.

- Board management will need to make a time and resource commitment to sustain the Boardwide planning effort, particularly as the process moves further into testing and developing more detailed procedures that affect all divisions and offices. Given the press of current business, Board officials will be challenged to invest resources in developing and testing response and recovery procedures absent a date-certain deadline such as the Y2K rollover. Senior managers will also need to commit time to review and discuss the protection strategy and plan evolving from the U. S. Secret Service vulnerability assessment to ensure a consensus of support for the results.

- Current organizational responsibilities may need to be reassessed. Responsibilities for continuity of operations planning and infrastructure protection operations presently reside in the Divisions of Information Technology and SS, and in the Office of Staff Director for Management, with the task force functioning as a Boardwide working group. This arrangement has worked reasonably well for planning efforts thus far because all groups ultimately report to the Staff Director for Management. When the Board's overall critical infrastructure and contingency plan is completed, however, the Board will likely need to consider how the critical infrastructure function should be organizationally structured to effectively implement the plan and transition to an operational function.

- Board and Reserve Bank coordination efforts will become even more important as the planning effort continues. The task force presently focuses on the coordination of critical infrastructure activities within the Board while the RBOPS BPP staff reviews such activities at Reserve Banks. As the Board's overall plan is developed, there will be areas—such as threat awareness communication, emergency operations status, and contingency facilities support—where coordination and support will be needed between the Board and Reserve Banks. Board management will need to ensure that the Board's and Reserve Banks' plans are effectively linked in these areas to provide a consistent Systemwide approach to critical infrastructure protection.

We have discussed the contents of this letter with the cognizant Board officials and staff and have incorporated their comments and suggestions. This report will be made available on our web page and copies will be furnished upon request. We have provided status information to the PCIE/ECIE review team for inclusion in their summary report. We would be happy to answer any questions you may have or to discuss the information contained in this report. We appreciate the excellent cooperation staff extended to us during this review.

Sincerely,

Barry R. Snyder
Inspector General

cc: Mr. Stephen Malphrus
Ms. Louise Roseman
Mr. Richard Spillenkothen